

## UNITED STATES DISTRICT COURT

for the  
District of Oregon

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*The person of William Warren Pearce and the premises  
located at 4696 SE Libby Ct., Hillsboro, Oregon 97123,  
more fully described in Attachment A

Case No. 3:20-mc-00606

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:The person of William Warren Pearce and the premises located at 4696 SE Libby Ct., Hillsboro, Oregon 97123, more fully described in Attachment A hereto,  
located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 18 USC Section 2252A	Transportation, Distribution, and Possession of Child Pornography

The application is based on these facts:

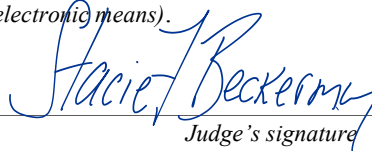
See the attached affidavit of FBI Task Force Officer Cheryl L. Banks.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days *(give exact ending date if more than 30 days: \_\_\_\_\_)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Cheryl L. Banks, Task Force Officer, FBI

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone at 9:33 a.m./p.m. *(specify reliable electronic means)*.Date: 6/18/2020City and state: Portland, Oregon

*Judge's signature*

Honorable Stacie F. Beckerman, U.S. Magistrate Judge

*Printed name and title*

**ATTACHMENT A**

**Description of Location to be Searched**

**The person of William Warren Pearce, born XX/XX/1965**



**The premises located at 4696 SE Libby Ct., Hillsboro, Oregon 97123, specifically common areas of the residence, any room rented, controlled, or used by William Pearce, and any area in which his belongings are stored.**

4696 SE Libby Ct., Hillsboro, Oregon 97123, is one half of a duplex. It is yellow with grey trim. The attached single car garage door is white. The numbers “4696” are attached to the right of the garage door.



## **ATTACHMENT B**

### **Items to Be Seized**

The following records, documents, and items that constitute contraband and evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Section 2252A, involving the transportation, distribution, and possession of child pornography.

1. Items to be searched for, seized, and examined:
  - a. All records, documents, or materials, including correspondence, pertaining to the production, transportation, distribution, receipt, possession of, or accessing with intent to view child pornography, as that term is defined in 18 U.S.C. § 2256;
  - b. All originals and copies of visual depictions of minors engaging in sexually explicit conduct as that term is defined in 18 U.S.C. § 2256, including photographs, images, and videos, whether in physical or digital form;
  - c. Computers, storage media, or digital devices, including cellular telephones, that were used or are capable of being used to commit the offenses described above, or to create, access, or store contraband or evidence, fruits, or instrumentalities of those offenses;
  - d. Evidence of internet usage for the transportation of, distribution of, possession of, or accessing with intent to view child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage, IP addresses, and screennames, user names, and passwords used to access the internet or any accounts via the internet;
  - e. Communications, including emails, chats, bulletin board posts, and comments relating to the production, transportation, distribution, receipt, possession of,

or accessing with the intent to view child pornography, to children engaged in sexually explicit conduct, and/or to a sexual interest in children;

f. All records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as that term is defined in 18 U.S.C. § 2256.

2. As used in this attachment, the terms “records,” “items,” “documents,” and “materials” include all of the foregoing items in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains, is capable of containing, or in which is stored records or information that is otherwise called for by this warrant (hereinafter “Computer”):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the internet.

### **Search Procedure**

4. The search for data capable of being read, stored, or interpreted by a computer or storage device may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain any digital device containing or constituting contraband or evidence, fruits, or instrumentalities of the offenses described herein, or to commence forfeiture proceedings against the device and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

I, Cheryl L. Banks, being duly sworn, hereby depose and state as follows:

1. I am a Detective employed by the City of Hillsboro Police Department and have been so employed since July 1993. I am also a Task Force Officer with the Federal Bureau of Investigation (FBI) and have been so assigned since October 2002. I am currently assigned to the Portland Division of the FBI where I investigate computer-related crimes. I have received training in the investigation of computer, telecommunications, and other technology crimes. Since October 2002, I have been involved in the investigation of matters involving the sexual exploitation of children, including the online sexual exploitation of children, particularly as it relates to violations of Title 18, United States Code, Sections 2251, 2252A and 2422. I am part of the Portland Child Exploitation Task Force (CETF), which includes FBI Special Agents and a Portland Police Bureau detective. CETF is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an online computer. As a member of this task force, I have received training and certification from the FBI in areas related to online computer crime investigation involving child pornography and other aspects of child exploitation.

2. I submit this affidavit in support of an application to search the person of William Warren Pearce, born XX/XX/1965, and the premises located at 4696 SE Libby Ct., Hillsboro, Oregon 97123, and in particular, the common areas of those premises and any room rented,



controlled, or used by Pearce (or in which his belongings are stored), as further described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), which prohibit transporting, distributing, receiving, and possessing child pornography. As set forth below, I have probable cause to believe that such items, further described in Attachment B, are currently on Pearce's person and in the common areas and rooms Pearce rents, controls, or uses at 4696 SE Libby Ct., Hillsboro, Oregon 97123.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The statements contained in this affidavit are based upon the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

#### **Applicable Law**

4. Title 18, U.S.C., § 2252A(a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or

foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term child pornography is defined in 18 U.S.C. § 2256(8).

### **Background on Computers and Child Pornography**

5. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

6. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

7. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives,

thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on someone's person.

9. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs such as LimeWire, eMule, and networks such as eDonkey, Gnutella, and BitTorrent, among others. Collectors and distributors of child pornography also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

10. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains

P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

11. P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. There are different software applications that can be used to access these networks, but many of these applications operate in essentially the same manner.

12. To access a P2P network, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a “shared” folder. All files placed in that user’s shared folder are available to anyone on the world-wide network for download.

13. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. The IP address is assigned by a user’s Internet Service Provider, and functions much like a telephone number, making it possible for data to be transferred between computers. An IP address can be statically assigned, meaning it is permanently assigned to a particular device or user and does not change from one Internet session to another. An IP address may also be dynamically assigned, meaning that a different number may be assigned to a particular user or device during each Internet session. Internet Service Providers typically log the subscriber to whom a particular IP address is assigned at any given time.

14. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest

in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

15. Importantly, evidence of such activity, including deleted child pornography, can often be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

#### **Background on the eDonkey Network and eMule**

16. P2P file sharing networks, including the eDonkey2000 network ("eD2K") and the Kademlia network ("Kad"), are used to trade digital image and video files containing child pornography. eMule is a free Microsoft Windows P2P client software program for the eD2k and Kad file sharing networks. eMule facilitates the direct exchange of files between clients and uses a credit system to reward frequent uploaders. The eD2k file sharing network is composed of users (also called "clients") and servers.

17. Typically, when a user launches the eMule client program, the program connects to an eD2K network server and sends the server information about the files the user is sharing. Such information may include the file's eD2k "hash value" (a digital fingerprint of sorts), the file's size, and parsed keyword terms from the file name. When a user wants to find a file on the eD2k network, the user enters a keyword search into the eMule search screen menu. The eD2k servers then search for files available for download from various client computers, and return the search results to the client who entered the search terms. Once a user identifies a file the user wants to download, the user manually initiates the download process, typically by double clicking on the desired file name. Users download the selected files directly from other users, not from the eD2K network servers.

18. Users follow similar steps when searching for and downloading child pornography files. Examples of common keyword search terms that locate child pornography include "PTHC" (pre-teen hard core), "babyj," "pedo," "kiddie," "underage," "child porn," "Vicky," and various terms relating to age such as "4yo" (4 years old).

19. Once a user chooses to download a particular file, the eMule client will again query the eD2k servers, although this query is not visible to the user. During this query, the eMule client will essentially ask for the IP addresses of other active clients that possess this file in whole or in part. The eMule client then uses the IP addresses to directly connect to another client (or clients) and to request the file. Typically, once the eMule client has downloaded part of a file, it may immediately begin sharing the file with other users.

20. In addition to the eD2k network servers, eMule clients can use Kad network protocols to locate files. Kad differs in that all communication is between clients, rather than

relying on servers. In general, the use of a Kad network versus an eD2k network server is invisible to the user. Typically, the Kad network and eD2K network operate in parallel to each other and assist in making P2P file sharing more efficient.

### **Law Enforcement Databases and Software**

21. I know that cooperating law enforcement agencies across the country pool their information to assist in identifying criminal conduct and building probable cause to further criminal investigations. Investigators around the country and around the world use automated tools designed by and for law enforcement to facilitate locating child pornography on eD2k, Kad, Bittorrent, and other P2P networks. Those tools identify files that a law enforcement officer has viewed and determined to contain child pornography (as defined by the laws in the officer's jurisdiction). Investigators are trained and licensed to use those tools to search for child pornography on those networks and to automatically submit their search results to centralized law enforcement-controlled and shared databases.

22. The data submitted to those databases include the hash values of child pornography files as well as the IP addresses offering to share those files. Investigators from around the world gather and log such information, which can be used to build probable cause in a specific case.

### **Statement of Probable Cause**

#### **I. Benton County Sheriff's Office Investigation of IP Addresses 50.39.170.32 & 50.39.168.129**

23. Detective Christopher Dale of the Benton County Sheriff's Office identified a device at IP address 50.39.170.32 as offering to share files believed to contain child pornography.

Between May 17, 2018, and November 28, 2018, Detective Dale downloaded 66 such files from that IP address. In January 2019, Detective Dale sent me the files on an encrypted DVD.

24. I reviewed the files and found that they contained child pornography. Descriptions of two of the downloaded videos follow:

a. A file, downloaded on May 17, 2018, contains a one minute video titled “6B74AA1D0F0450EDE8896F34B2A92F83.” The video depicts a nude prepubescent girl positioned between the legs of a naked adult man. The man tells the girl to suck on his penis. The child reluctantly places her mouth on the man’s penis.

b. A file, downloaded on November 28, 2018, contains a two minute video titled “BD5FF55D21DF36E125B05F4DCD6300FB.” The video depicts a prepubescent girl wearing only a pink colored top. An adult man inserts his penis into the child’s anus then ejaculates onto her vaginal area.

25. Between January 14, 2019, and February 3, 2019, Detective Dale downloaded additional files containing child pornography from IP address 50.39.170.32. In March 2019, he sent me another encrypted DVD containing those files. I reviewed the files and found that they contained child pornography. Descriptions of two of the files follow:

a. A file downloaded on January 14, 2019, contains an image titled “6C4BD40B8701771079C990BDEF33620,” which depicts a prepubescent girl performing oral sex on an adult man.

b. A file downloaded on February 3, 2019, contains a 2 minute video titled “5D095D3D533A094C5FCECA49FE569A5D,” which depicts a prepubescent girl performing oral sex on an adult man.

26. IP address 50.39.170.32 belongs to Frontier Communications. I sent administrative subpoenas to Frontier seeking subscriber information for that IP address for May 17, 2018, November 28, 2018, and February 3, 2019 (dates on which Detective Dale downloaded child pornography from that IP address). In response to the subpoenas, Frontier provided the following information:



Subscriber Name: Jack Lee  
Service Address: 4696 SE Libby Ct., Hillsboro, Oregon 97123  
Telephone #: 503-640-0529  
Start: 2017-10-18 21:24:46 UTC (Still Active)

27. On May 12, 2020, Homeland Security Investigations (HSI) Special Agent Clinton Lindsly contacted me concerning IP address 50.39.168.129, which he was investigating in connection with the distribution of child pornography. SA Lindsly provided me with the following subscriber information for that IP address, which he received from Ziply, formerly known as Frontier Communications:

IP Address: 50.39.168.129  
Session Start: 2019-10-08 22:38:20 UTC  
Customer name: Jack Lee  
Account Address: 4696 SE Libby Ct., Hillsboro, Oregon  
Billing Address: Same  
Billing telephone: 503-640-0529  
Contact Number: 503-560-0821 and 503-985-2083  
Length of Service: 10/18/2017 to Present  
Account Status: Active  
Email Address: [jacklee21010@frontier.com](mailto:jacklee21010@frontier.com)  
[jcllee@yahoo.com](mailto:jcllee@yahoo.com)  
[apmgr@outlook.com](mailto:apmgr@outlook.com)  
[beckylee90@gmail.com](mailto:beckylee90@gmail.com)

180 day IP History: Has had IP address 50.39.168.129 since 2019-10-08 22:38:20 UTC

28. Between October 28, 2019, and April 5, 2020, Detective Dale downloaded or partially downloaded approximately 40 files believed to contain child pornography from IP address 50.39.168.129. Detective Dale provided me with an encrypted link which contained the files he downloaded. On May 27, 2020, I reviewed the files and determined that 16 of the 40 files contained images or videos depicting child pornography. Descriptions of some of those files follow:

a. A file downloaded on November 05, 2019, contains a 22 minute video titled “15056B76F33EA0AC3237FBA070DD1282.mpg.” The video depicts a boy, about 12-14 years old, removing his clothing. The boy is laying on a bed massaging his penis. An adult man begins to rub the boy’s penis. The video then shows the boy masturbating. The boy then rubs and sucks on the adult’s penis.

b. A file downloaded on January 19, 2020, contains a one minute video titled “C7992A009AD088B8A8AACD6A941C7929.mp4,” which depicts a nude prepubescent girl positioned on a bed next to an adult man. The man masturbates and ejaculates while holding on to the child.

c. A file downloaded on February 1, 2020, contains an image titled “D3B6D28C0B8696FED6F32535B2A5Cf72.jpg,” which depicts a barely pubescent nude girl sitting on a brown chair with her legs spread and what appears to be a white vibrator inserted in her vagina. The child appears to have an injury on her right knee.

d. A file downloaded on March 20, 2020, contains an image titled “5717B263CE84CBA073E79776ADB79.jpg,” which contains screen captures from a video showing an adult man, an adult woman, and a nude prepubescent girl. The adult woman is seen inserting her finger into the girl’s vagina, and the man’s penis is seen on the child’s vaginal area.

e. A file downloaded on April 5, 2020, contains a 13 minute video titled “3BFB233A3075492FE258982F328E29FB.mpg,” which depicts a nude prepubescent male or female child and two nude males, one of whom appears to be a prepubescent child, and one who appears to be an adult. The males are positioned on their hands and knees (anuses exposed) facing away from the camera. The male or female child is positioned between the two males and is seen rubbing each one’s penis. The male or female child inserts his/her fingers into the anus of each male. The adult male then inserts his penis into the anus of the male child.

## **II. FBI Investigation and Surveillance**

29. While standing directly in front of 4696 SE Libby Ct., Hillsboro, Oregon 97123 on March 12, 2019, I observed numerous Wireless Access Points (WAPs) in the area. None of them were open. All were listed as secure. In order to use any of those wireless access points to access the Internet, a user would have to know the encryption code or security key for that particular account.

30. In March 2019, May 2020, and June 2020, I conducted physical surveillance at 4696 SE Libby Ct., and saw several vehicles registered to different people at various addresses parked in front of the house.

a. On March 12 and 14, 2019, I saw three vehicles parked in front of the premises: (1) a light brown 2014 Toyota utility vehicle, Oregon license plate 302HVN, registered to Wenchuang Qui at 4696 SE Libby Ct., Hillsboro, Oregon 97123; (2) a silver 2003 Ford Mustang, Oregon license plate 512GVV, registered to Rebecca Dawn Lee at 4696 SE Libby Ct., Hillsboro, Oregon 97123; and (3) a silver 2011 Dodge Dakota, Oregon license plate 730LGE, registered to Roger Alan Quartaro at 4696 SE Libby Ct., Hillsboro, Oregon 97123. An NCIC query did not reveal any criminal history for Wenchuang Qui, Rebecca Dawn Lee, Roger Quartaro or Jack Chang Dok Lee, who owns the premises. Jack Chang Dok Lee's Oregon driver's license lists his address as 3000 SW 192<sup>nd</sup> Avenue, Beaverton, Oregon, and 2850 SW Cedar Hills Blvd., #339, Beaverton, Oregon.

b. On May 21 and 26, 2020, I saw two vehicles parked in front of the premises: (1) a yellow 2003 Dodge Neon, Oregon license plate 409LZV, registered to William Warren Pearce at 4696 SE Libby Ct., Hillsboro, Oregon 97123; and (2) a grey 2005 Nissan Sentra with Oregon license plate 445CDD, registered to James Alfred Lee and Diane Pearl Lee at 3318 E Main St., Hillsboro, Oregon 97123. An NCIC query revealed that William Pearce was arrested by the Hillsboro Police Department on January 14, 2009, for Negotiating a Bad Check and Theft in the First Degree. The charges were later dismissed. An NCIC query revealed no criminal history for James or Diane Lee.

c. On June 2, 2020, I saw a 2003 Mazda B3000, with Oregon license plate 960FHQ, registered to Timothy Douglas MacMillan at 6798 SE Reedville Creek Dr., Hillsboro, Oregon 97123. An NCIC query did not reveal any criminal history for Timothy MacMillan.

31. 4696 SE Libby Ct., Hillsboro, Oregon 97123, is one half of a duplex. It is yellow with grey trim. The attached single car garage door is white. The numbers “4696” are attached to the right of the garage door. 4696 SE Libby Ct. is owned by Jack Lee, who rents out rooms to four individuals, as described below.

### **III. Additional FBI Investigation**

32. On June 5, 2020, I spoke with Jack Chang Dok Lee, who told me he owns the premises located at 4696 SE Libby Ct., Hillsboro, Oregon 97123. Lee identified himself as the “landlord” of the property, and said three women and one man currently live there. Each person pays rent and has one bedroom (living area). The residents do not have access to each other’s living areas. Lee said there are “common” areas within the residence, such as the living room and kitchen, to which each resident has access. Lee identified Rebecca Lee (no relation) as the “principle tenant,” and three “sub-tenants” who rent from her. Lee said although he is aware of who lives at the residence, he is not necessarily friendly with them and does not communicate with them on a regular basis.

33. Lee said the Internet Service Provider (ISP) for 4696 SE Libby Ct. used to be Frontier Communications, but is now Ziply. Lee is the subscriber and pays the Internet bill.

34. I asked Lee about the male tenant. Lee was reluctant to provide information. I showed him a Department of Motor Vehicles (DMV) photograph of Timothy MacMillan. Lee said he didn’t recognize him. When I showed Lee a DMV photograph of William Pearce, Lee

said, “Yes.” Lee said he believes Pearce has continuously lived at 4696 SE Libby Ct. for about three years. Lee estimated that Pearce moved in sometime in 2017.

35. A query of the Oregon DMV database shows that William Pearce received a change of address sticker for his driver’s license on August 8, 2017. Pearce’s driver’s license lists his address as 4696 SE Libby Ct., Hillsboro, Oregon 97123.

36. I have since learned that James Alfred Lee and Diane Pearl Lee reside at 3318 E Main St., Hillsboro, Oregon 97123. I believe they are the parents of Rebecca Lee. Wenchuang Qui, Roger Quartaro and Jack Lee no longer reside at 4696 SE Libby Ct. Pearce and Rebecca Lee are the only ones who have lived continuously at that address during all of the times Detective Dale downloaded child pornography from a computer whose IP address is registered there.

#### **Search and Seizure of Digital Data**

37. This application seeks permission to search for particular items, described in Attachment B, which will likely be found on Pearce’s person and in the residence described in Attachment A, in whatever form those items may be found. One form in which that evidence will likely be found is as data stored on a computer’s hard drive, on other digital storage media, or on other digital devices, including cell phones. Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).

38. I have probable cause to believe that the items described in Attachment B will be stored on one or more digital device(s), based on the foregoing facts and on my knowledge, training, and experience that:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files may reside in free space or slack space – that is, in space on the digital device that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices – in particular, internal hard drives – contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. For example, forensic evidence can take the form of operating system configurations, artifacts from the operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

39. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also forensic electronic evidence that establishes how digital devices were used, the purpose

of their use, who used them, and when. I have probable cause to believe that this forensic electronic evidence will be on any digital device on Pearce's person and in any rooms rented, controlled, or used by Pearce (or in which his belongings are stored) in the residence described in Attachment A, because, based on my knowledge, training, and experience, I know:

a. Data on a digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic

analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. In addition, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device, or password-protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.



e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a digital device to commit a crime such as the child pornography offenses described herein, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of the crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

40. In most cases, a thorough search of premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device

and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. Not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

41. Because it appears that at least one other person resides at the premises, it is possible that the premises will contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is

possible that the things described in this warrant could be found on any of those digital devices (e.g., that Pearce had access to and used devices belonging to others), the requested warrant would permit the seizure and review of those items as well.

42. *Nature of the examination.* Based on the foregoing, and consistent with Fed. R. Crim. P. 41(e)(2)(B), the warrant for which I am applying would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and Attachment B, and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including computer-assisted scans of the entire device that might expose many parts of a hard drive to human inspection in order to determine whether it contains material subject to seizure and search under the warrant.

43. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of that time period from the Court.

44. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data

falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

45. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

46. The government may retain any digital device containing contraband or evidence, fruits, or instrumentalities of the offenses described above and in Attachment B, or to commence forfeiture proceedings against the device and/or the data contained therein.

47. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

48. The government has not made any prior efforts in other judicial fora to obtain the evidence sought under the warrant.

### **Conclusion**

49. Based on the foregoing information, I have probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), as set forth herein and in Attachment B, are

currently on the person of William Warren Pearce and at the residence located 4696 SE Libby Ct., Hillsboro, Oregon 97123, more specifically within the common areas of the residence and any room rented, controlled, or used by Pearce (or in which his belongings are stored), as described in Attachment A. I therefore respectfully request the Court issue a warrant authorizing a search of Pearce's person and the premises described in Attachment A for the items described above and in Attachment B, and the seizure and examination of any such items found.

50. This affidavit, the accompanying application, and the requested search warrant were reviewed by Assistant United States Attorney Gary Sussman prior to being submitted to the Court. AUSA Sussman informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By phone

---

CHERYL L. BANKS  
Task Force Officer  
Federal Bureau of Investigation

Sworn to before me telephonically this 18th day of June 2020 at 9:33 pm.


---

HONORABLE STACIE F. BECKERMAN  
United States Magistrate Judge